IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

UNITED STATES OF AMERICA	§	
	§	
v.	§	No. 3:09-CR-210-B
	§	
JESSE WILLIAM MCGRAW (1)	§	
also known as Ghost Exodus	§	

FACTUAL RESUME

Jesse William McGraw, John Nicholson, the defendant's attorney, and the United States of America (the government), agree that the following accurately states the elements of the offense and the facts relevant to the offense to which the defendant is pleading guilty:

Elements:

1. In order for the defendant to be convicted at trial of a violation of 18 U.S.C. §1030(a)(5)(A) and §1030(c)(4)(B)(i)(II) (and in Count Two §1030(c)(4)(B)(i)(IV)), the United States would have to prove each of the following elements of the offense beyond a reasonable doubt:

First: That McGraw, through means of a computer used in interstate commerce or communications, knowingly caused the transmission of a program, information, code, or command to another computer or computer system, as charged;

Second: That McGraw, by causing the transmission intended to damage the receiving computer, computer system, information, data or program, and withhold or deny, or cause the withholding or denial, of the use of a computer, computer services, system, or network, information, data or program;

Third: That McGraw so acted without the authorization of the persons or entities who own or are responsible for the computer system receiving the program, information, code, or command; and

Fourth: That McGraw's acts potentially modified or impaired, the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals; *and*

for Count Two
Fifth: That McGraw's acts potentially created a risk to public health and safety.

Facts:

1. From October 30, 2008, until June 26, 2009, McGraw was employed as a security guard for United Protection Services, a security firm in Dallas, Texas. From November 1, 2008, until June 26, 2009, McGraw was assigned by United Protection Services to work security at the North Central Medical Plaza, located at 9301 North Central Expressway, Dallas, Texas. The North Central Medical Plaza housed medical offices and surgery centers, to include the W.B. Carrell Memorial Clinic[1] and the North Central Surgery

[1] The W. B. Carrell Memorial Clinic provides comprehensive orthopaedic care by board certified orthopaedic surgeons and staff.

Center[2]. Generally, McGraw's shift was Thursday through Tuesday, from 23:00[3] until 07:00. McGraw's assignment constituted a position of trust.

2. The following computers (or computer systems) were located within the North Central Medical Plaza, and constituted protected computers pursuant to 18 U.S.C. §1030(e)(2), in that they were used in or affecting interstate commerce or communications.

a. The Nurses Station E computer had the host name WBCCW125 and was located on the 5th floor of the North Central Medical Plaza. The computer was used to track a patients progress through the W.B. Carrell Memorial Clinic. Medical staff also used the computer to reference a patient's personal identifiers, billing records, and medical history.

b. The HVAC computer was located in a locked room of the North Central Medical Plaza and was used by the building engineering staff. The HVAC computer was used to control the Heating Ventilation and Air Conditioning for the first and second floors used by the North Central Surgery Center.

3. McGraw gained physical access to approximately 14 computers located in the North Central Medical Plaza, including the two identified above. McGraw installed (transmitted) "Logmein," an application program that allows remote access to those

---

[2] The NCSC provides state-of-the-art equipment for surgeons to perform procedures in the speciality areas of General Surgery; Gastroenterology (GI); Gynecology; Ophthalmology; Orthopedic; Pain Management; Plastic Surgery; Podiatry; Ear, Nose and Throat; Bariatric; Spine; and Urology.

[3] All time will be referenced in military time.

computers. The Logmein installation bypassed existing security protocols put in place by the owners and compromised the integrity of these computer systems and the associated network by allowing remote access by unauthorized individuals. McGraw also impaired the integrity of the computer systems by removing security features, e.g. uninstalling anti-virus programs, which made the computer systems and related network more vulnerable to attacks. McGraw also installed a malicious code and program, sometime called a "bot", which was used to remotely access and control the compromised computer. "Bots" are usually associated with theft of data from the compromised computer, using the compromised computer in denial of service attacks, and using the compromised computer in sending SPAM. McGraw installed the "bot" known as "RxBot" on the compromised computers and controlled the compromised computers from websites under his control, specifically eta.myvnc.com and eta2.myvnc.com.

4. McGraw intended to impair the integrity of the accessability of the computers and computer systems, by turning off the security protocols, and by creating a means by which he could remotely access the computers and computer systems. Therefore, by installing (transmitting) the Logmein program and the RxBot program, McGraw damaged and intended to damage the computers or computer systems as defined by 18 U.S.C. §1030(e)(8).

5. McGraw knew that these actions would damage the security and integrity of these systems. McGraw advocated taking these kinds of actions in order to adversely affect the integrity of systems and avoid detection, in instructions that he posted online for members

of his “Electronik Tribulation Army” (ETA) and other individuals interested in committing fraud against computers.

6. On or about February 12, 2009, McGraw abused the trust placed in him as a security guard and bypassed the physical security to the room in the North Central Medical Plaza containing the HVAC computer. At approximately 23:35, McGraw without authorization began the download (transmission) of "Ophcrack-vista-livecd-2.1.0.iso," a malicious password cracking tool from the website sourceforge.net. McGraw then downloaded and installed (transmitted) without authorization Team Viewer 4, a remote access program. McGraw then circumvented the security software McAfee and added Teamviewer to the list of allowed programs in McAfee. By February 13, 2009, at approximately 01:19 McGraw again without authorization physically accessed the HVAC computer and inserted a removeable storage device named "HARD DISK X" and executed the program daemon4301-lite.exe which allowed McGraw to emulate a CD/DVD device with the removeable storage device. McGraw used "Sonic Record Now," a CD/DVD burning software, to create a bootable CD image using a previously downloaded "OphCrack-xp-livecd.iso".

7. On or about April 28, 2009, at about 01:47, McGraw abused the trust placed in him as a security guard and accessed without authorization the Nurses Station E computer. McGraw inserted into the computer a CD containing the OphCrack program to bypass any passwords or security, disengaged the McAfee VirusScan Enterprise program

which turned off the existing security features making it more vulnerable to attack, and installed (transmitted) RxBot, the malicious code or program.

8. On or about April 7, 2009, at approximately 02:30, McGraw abused the trust placed in him as a security guard and bypassed the physical security to the room in the North Central Medical Plaza containing the HVAC computer. At approximately 03:12, McGraw installed (transmitted) Logmein to the HVAC computer.

9. On or about the following dates, McGraw remotely accessed without authorization the HVAC computer:

DATE	TIME	DURATION
04/13/09	07:21	5m:43s
04/13/09	07:24	2m:37s
04/13/09	20:09	55m:31s
04/14/09	06:50	2m:38s
04/14/09	06:56	14m:15s

10. On April 13, 2009[4], McGraw without authorization remotely accessed the HVAC computer using the password "pred818" and downloaded and installed (transmitted) the malicious program "Cain & Abel v4.9.29", a key stroke logger and network traffic sniffer. A keystroke logger is a program that covertly records and captures all keystrokes. A network traffic sniffer is a program that covertly intercepts and logs traffic passing over a

[4] This April 13, 2009 remote access may or may not be the same as noted in paragraph 9. As of the time of the drafting of the Factual Resume, the FBI could not determine a time

digital network or part of a network. On April 13, 2009, McGraw used the "Cain" software to access the HVAC computer's Local Security Authority also known as "LSA secrets." The HVAC computer's LSA stored the cached user authentications.

11. McGraw was not authorized, and knew that he was not authorized, to physically or remotely access any of these computers or computer systems located within the North Central Medical Plaza. McGraw was not authorized, and knew that he was not authorized, to transmit any programs, codes, or command to these computers or computer systems.

12. McGraw was aware that some of the computers he compromised, such as the Nurses Station E computer, were used to access and review medical records. By gaining administrator access to these computers, McGraw had the ability to modify these records.

13. McGraw was aware that the HVAC computers were used to maintain the environmental controls in the facility. He knew that by modifying these controls he could affect the temperature of the facility. By affecting the environmental controls of the facility, he could have affected the treatment and recovery of patients who were vulnerable to changes in the environment. In addition, he could have affected treatment regimes, including the efficacy of any or all of the temperature sensitive drugs.

14. McGraw understands that the cost to remediate the compromised computers and computer systems with the North Central Medical Plaza exceeded $30,000, but was less than $70,000.

JAMES T. JACKS
UNITED STATES ATTORNEY

_____ _____
CANDINA S. HEATH Date
Assistant United States Attorney
Texas State Bar No. 09347450
1100 Commerce Street, Third Floor
Dallas, Texas 75242-1699
Tel: 214.659.8600
Fax: 214.767.2846
candina.heath@usdoj.gov

I have read (or had read to me) this Factual Resume and have carefully reviewed every part of it with my attorney. I fully understand it and I swear that the facts contained herein are true and correct.

_____ _____
JESSE WILLIAM MCGRAW Date
Defendant

I am the defendant's counsel. I have carefully reviewed every part of this Factual Resume with the defendant. To my knowledge and belief, my client's decision execute this Factual Resume is an informed and voluntary one.

_____ _____
JOHN NICHOLSON Date
Attorney for Defendant